for Servers

SafeNet ProtectDrive™

User Manual

© 2012 SafeNet, Inc. All rights reserved.

Part Number 007-011121-001 (Rev E, August 2012)

Software Version 9.4.2

All intellectual property is protected by copyright. All trademarks and product names used or referred to are the copyright of their respective owners. No part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, chemical, photocopy, recording or otherwise without the prior written permission of SafeNet.

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person or organization of any such revisions or changes.

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

SafeNet invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be sent to the address below.

SafeNet, Inc.
4690 Millennium Drive
Belcamp, Maryland 21017
USA

Technical Support

If you encounter a problem while installing, registering or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, please contact your supplier or SafeNet support. SafeNet support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between SafeNet and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Technical Support Contact Information:
Phone: 800-545-6608
Email: support@safenet-inc.com

Acknowledgements

- ProtectDrive includes software developed by Apache Software Foundation (http://www.apache.org/).
- Windows is a registered trademark of Microsoft Corporation in the United States and other countries.
- Windows Vista is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries.
- Windows 7 is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries.

Relevant Documentation

Basic configuration procedures for token support are discussed in this manual. For detailed installation and configuration information relevant to SafeNet's Borderless Security tokens, please refer to the following documents:

- *Borderless Security PK and SSO Administration Guide*
- *Borderless Security PK and SSO User Guide*

Table of Contents

Chapter 1 Introduction 1
Product Overview 1
Who Should Read This Document? 3
Chapter 2 Logging In to Your ProtectDrive-secured PC 5
Overview 5
Default Pre-boot Login Screens 5
Legacy Login Screens 7
Auditory Prompting 8
Helpful Hints 10
Logging In With Smart Card/Token and PIN 11
Logging In With Smart Card/Token and Fingerprint 11
Logging In With User ID/Password/Domain 12
What to Do If Your Pre-boot Login Fails 12
Incorrect Pre-boot Username and/or Password 12
Pre-boot Login Failure Due to System Inoperability 12
Chapter 3 Logging In to Windows 13
Manual Windows Login 13
Logging In to Windows With Smart Card/Token and PIN 14
Logging In to Windows with User Name/Password/Domain 14
Logging In to Windows with Smart Card/Token and Fingerprint 15
Chapter 4 Using Windows with ProtectDrive 17
ProtectDrive User Authentication Activity Tracking 17
Disk Encryption Warning 18
Windows Shrink Volume Feature 18
SafeNet ProtectDrive Notification Area Icon 18
Access the Local Management Console 19
Lock the Windows Desktop 20
Register a Shared Key 20
View About SafeNet ProtectDrive Information 23
Using the Windows Folder Compression Application on Your ProtectDrive-secured PC 24
Using the Windows System Restore Utility on Your ProtectDrive-secured PC 24
Changing Your ProtectDrive Pre-boot Password 24
Disallowed Device Access Errors 25
Backing Up the License File 25
Chapter 5 Encrypting Hard Drives & Removable Media 27
Encrypt a Hard Drive 27
Decrypt a Drive 30
Re-encrypt a Drive Using a Different Algorithm 30
Removable Media 31
Encrypt Removable Media 31

Automatic Prompt to Encrypt *31*
Windows Explorer Encrypt Media Option *32*
Lock Removable Media 34
Unlock Removable Media 34
Decrypt Removable Media 35
Repair Removable Media 36
Standard Recovery Procedure *36*
Alternate Recovery Procedures *37*
Recover Removable Media 38
End User Instruction—Generate a Challenge Code *38*
System Administrator Instruction—Generate a Recovery Response Code *39*
End User Instruction—Reset the Removable Media Password *40*

Chapter 6 Configuring ProtectDrive Users 42

Set Device Access Control Permissions for a User 43
Add a ProtectDrive User 43
Change a ProtectDrive User's Initial Password 44
Remove a ProtectDrive User 44

Chapter 7 Troubleshooting 45

What to Do If You Misplace Your Smart Card/Token or Forget Your PIN 45
What to Do If You Forget Your Password 46
What to Do If You Do Not Have a Pre-boot User Account 47
Emergency Logon Without Username Procedure *48*

 © SafeNet, Inc.

Chapter 1
Introduction

Product Overview

In today's computing environment, hard disk drives (HDD) have become mass repositories of proprietary information. The widely used Windows operating systems provide adequate data privacy, whether on a stand-alone machine or a networked computer (in most operating environments). However, insufficient data security protection exists in a case of system (or HDD) loss due to malicious intent. Unless appropriate data protection measures are taken, any HDD can be removed from the system, and data on it may be read.

One of the PC security functions provided by ProtectDrive is *User Authentication* (login) into the system. This is a two-stage sequential process as follows:

Pre-boot User Authentication (32-bit pre-boot is the default)

The user is required to provide valid login credentials right after the computer is turned on and *before* Windows loads. Login methods are discussed on the next page. Support for auditory prompting during pre-boot authentication for the visually impaired is also available (for example, prompts occur for a number of screen states or conditions, such as smart card or token insertion, successful logon, and unsuccessful logon. For details, refer to the *ProtectDrive Administration Guide*).

Windows Authentication

This is the actual Windows login based on the user's Windows authentication methods in existence prior to the ProtectDrive installation.

Generally, ProtectDrive will be configured by the System Administrator to perform the Windows login *automatically*, requiring no user input.

In isolated cases, however, the user may be required to log in to Windows separately following their ProtectDrive (Pre-boot) login.

The above two methods of user authentication typically rely on the user's existing Windows login credentials, which are configured by the System Administrator. There are two distinct login methods:

Smart Card/Electronic Token/PIN/Fingerprint	With this method, the user inserts a smart card into a reader and then types in their PIN or scans their fingerprint on a biometric reader. Alternatively, the user may insert a token into the USB port and then type in their PIN.
User ID/Password/Domain	With this method, the user types in their Windows username (User ID), password, and domain name.

Users will need to contact their ProtectDrive System Administrator for detailed instructions on how to log in to their respective systems.

For a list of supported tokens and smart cards, refer to the *ProtectDrive Administration Guide*.

© SafeNet, Inc.

Who Should Read This Document?

This document is intended for computer end users who use their PC systems for everyday operations, such as word processing, e-mail, Internet access, etc.

The scope of this document assumes that your computer is managed by an IT professional—this would typically be your System Administrator. This person is generally responsible for configuration and maintenance of various computer system components such as ProtectDrive.

This user document assumes ProtectDrive is already installed and ready to use. It introduces basic ProtectDrive operation from the end user perspective, and covers ProtectDrive operational issues, such as:

- How to turn on and log in to your ProtectDrive-secured PC
- How to log in to Windows on your ProtectDrive-secured PC
- What to do if you misplace your smart card/token or forget your PIN
- What to do if you forget your password
- What to do if your login fails
- How to use Windows with ProtectDrive
- How to perform hard drive encryption
- How to perform removable media encryption

Minimal technical knowledge is required to digest this material. Please consult your System Administrator and the latest version of the *ProtectDrive Administration Guide* for issues pertaining to ProtectDrive installation, data encryption, system and user management, and disaster recovery.

THIS PAGE INTENTIONALLY LEFT BLANK

© SafeNet, Inc.

Chapter 2
Logging In to Your ProtectDrive-secured PC

Overview

When the ProtectDrive-secured PC is powered on, it will boot normally. The first screen that displays will depend on how ProtectDrive is configured to allow users to log in to the PC.

The default (high resolution) pre-boot screens shown in the following examples have a black background. If high resolution is not supported, then the pre-boot screens have a white background, which is typical of the legacy pre-boot screens shown on page 7. These low resolution screens function virtually the same as their high resolution counterparts. Please note the following:

- Legacy pre-boot screens do not support fingerprint logon or auditory prompting.
- If both Password Domain and Token Domain authentication options are configured, the legacy screens do not include an initial pre-boot screen (shown in the first example below), which allows the user to choose the login method. Instead, the user can press the **[F2]** function key to toggle between these two login screens.

Default Pre-boot Login Screens

When the computer is started, an initial pre-boot screen displays if the system is configured to allow either *User ID/Password/Domain* login or *Smart Card/Token and PIN/Fingerprint* login. If a PIN-only login is allowed, then this screen does not display. If the wrong login method is selected here, press **Esc** to return to this initial screen.

Figure 1- Initial Pre-boot Screen—choose login method

The following screen displays after the user presses **Enter** to access the *Username/Password/Domain* login screen (Figure 2). If smart card or token login is required instead, refer to Figures 3 and 4.

Figure 2 – User ID/Password/Domain Log On

The following screen displays if smart card/token login requires a PIN entry and/or a biometric (fingerprint) reader is not detected (Figure 3). If smart card/token login requires a fingerprint instead of a PIN entry, refer to Figure 4.

Figure 3 - Smart Card/Token/PIN Login

© SafeNet, Inc.

The following screen displays if smart card/token login requires a fingerprint, the inserted smart card or token is fingerprint-enabled, *and* a biometric reader is detected. PIN entry is an alternative login method on this screen (Figure 4).

Figure 4 – Smart Card/Token/Fingerprint (or PIN) Login

Legacy Login Screens

Fingerprint authentication and auditory prompting are not supported on legacy screens.

When the PC is started, the following screen displays if the system is configured to allow *User ID/Password/Domain* login (Figure 5). If smart card or token login is required instead, refer to Figure 6.

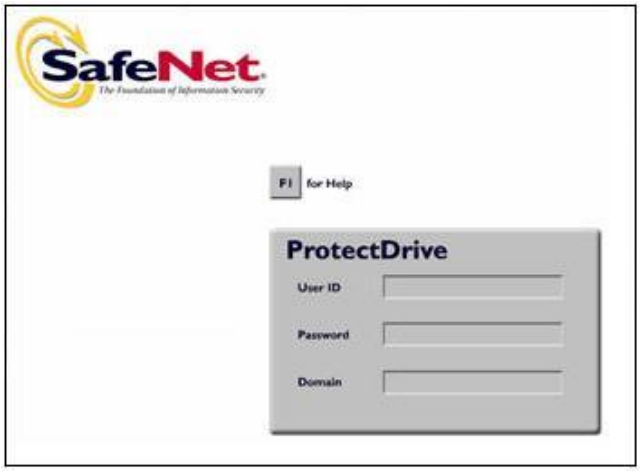


Figure 5 – User ID/Password/Domain Login

When the PC is started, the following screen displays if the system is configured to allow *Smart Card/Token PIN* login (Figure 6).

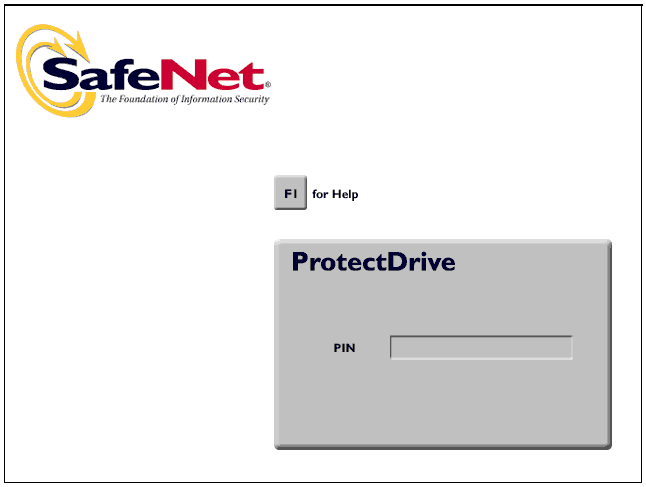


Figure 6 - Smart Card/Token/PIN Login

Auditory Prompting

Auditory prompts are intended to be used by visually impaired users. When this feature is enabled, audio prompts will occur for a number of screen states or conditions during the pre-boot login process.

Each audio prompt consists of a series of short or long beeps, or a combination of both. Refer to the table on the next page for a description of each audio prompt and the condition under which it will occur.

Audio prompting is available on 32-bit pre-boot user authentication only (it is not supported for legacy pre-boot authentication).

To enable auditory prompting, press **F3** from any pre-boot login screen. To toggle the feature off, press **F3** again. The auditory prompting feature can also be enabled through the Local Management Console. For details, refer to the *ProtectDrive Administration Guide*.

When audio prompting is enabled, press **F4** to replay the audio prompt for the current field or condition.

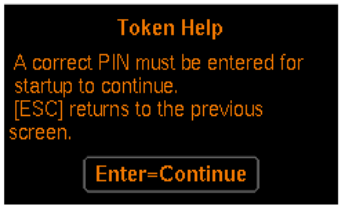
If the user is unable to determine where they are in the login process, press **Esc** to return to the initial pre-boot screen. (This is only applicable if both password and token authentication methods are enabled.)

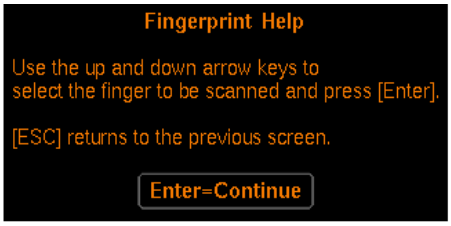
© SafeNet, Inc.

This pre-boot prompt, state, or condition…	…emits this audio prompt…	…which equates to these musical notes…	…and you should:
Insert the smart card/token or press Enter (**Note**: This screen displays only if both password and token authentication methods are enabled. If only one method is enabled, the first audio prompt the user hears will either be for user name entry, which is 2 short beeps, or for PIN entry, which is 3 short beeps.)	1 long beep	A	Insert a smart card/token or press **Enter** to continue.
Enter the user name (User ID)	2 short beeps	B, B	Enter your user name and press **Tab** to continue.
Enter the password	3 short beeps	C, C, C	Enter your password and press **Tab** to continue.
First domain in the list is selected	4 short beeps	D, D, D, D	Press **Enter** to select the first domain in the list to continue, or press the down arrow to select a different domain.
Press the up/down arrow to choose a different domain (**Note**: One short beep will occur with every press of the up/down arrow. If the first domain is reached again, 4 short beeps will sound to indicate the user is at the top of the domain list.)	1 short beep	E	Press **Enter** to continue.
Enter the PIN	3 short beeps	C, C, C	Enter your PIN and press **Enter** to continue.
Logon is successful	1 long beep, 3 short beeps	G, D, B, A	None
A pop-up box is displayed, as a result of the user's last action. The pop-up box describes feedback such as: • A general entry error occurred (for example, an invalid user name, password, PIN, smart card, or bad certificate). • The user pressed **F1** which displays a login help screen	1 short beep, 1 long beep	B, D	Press **Enter** to clear the pop-up box and continue. • If the condition occurred while entering a user name or password, continue by re-entering that information. • If the condition occurred while entering a PIN, continue by re-entering a correct/valid PIN, or by replacing the card with one that works.
Challenge/response screen is active	2 long beeps	A, A	Contact your administrator for recovery instructions.
Lockout screen is displayed The user has reached the number of failed log in attempts and is now locked out for a period of time.	2 beeps, 1 long beep	B, B, F	Press **Enter** to acknowledge the message and wait the configured amount of time to attempt login again.
Critical/fatal error	3 short beeps, 1 long beep	B, B, B, F	Contact your administrator.

Helpful Hints

- (Legacy pre-boot screens only) If the system has been configured to allow *Smart Card/Token/PIN* access, as well as *User ID/Password/Domain* access, press the **[F2]** function key to switch from one login method to the other.
- (Default pre-boot screens only) A blank screen saver will automatically take effect when a workstation is left unattended for at least 10 minutes.
- From either type of pre-boot login screen (*User ID/Password/Domain* or *PIN/Fingerprint*), press the **[Esc]** key to return to the previous screen.
- Press the **[F1]** function key to display **Help** from any pre-boot login screen. A few examples are shown below.




Fingerprint Help
Use the up and down arrow keys to select the finger to be scanned and press [Enter].
[ESC] returns to the previous screen.
Enter=Continue

© SafeNet, Inc.

Logging In With Smart Card/Token and PIN

After the system has been turned on, to log in:

1. Insert the smart card or token into the reader.
2. Type your PIN.
3. Press **Enter**.

The Windows desktop displays. Unless you are logging in with a *shared key* token, in most common ProtectDrive configuration scenarios, the system will log the user in to Windows *automatically*. However, in isolated instances, the System Administrator may configure ProtectDrive to require the user to log in to Windows manually.

Windows login is *always* required if you log in with a *shared key* token. Refer to Chapter 3 – Logging In to Windows.

Logging In With Smart Card/Token and Fingerprint

Single sign-on is currently not supported with fingerprint login, which means you will not be automatically logged in to Windows after you've successfully logged in to ProtectDrive.

Up to four fingerprints can display during the login procedure. The number of selections depends on the number of fingerprints that were enrolled during smart card/token configuration. Refer to the *SafeNet Borderless Security PK and SSO User Guide* for details on fingerprint enrollment.

After the system has been turned on, to log in:

1. Insert the smart card or token into the reader.
2. Select the finger to be scanned from the **Finger** drop-down list. (As an alternative, the user can enter a PIN instead of scanning their finger.)
3. Press **Enter**.
4. When the *Position Finger* prompt displays, place your finger on the biometric reader. The reader will process the fingerprint to verify that it matches one that is linked to the card.
5. When the verification process is complete (the fingerprint is accepted), the scanned fingerprint displays.
6. Before the Windows desktop displays, you will be prompted to place your finger on the biometric reader again. Follow the instructions on the screen to complete the login procedure. (Refer to page 15 for more details.)

Logging In With User ID/Password/Domain

After the system has been turned on, to log in:

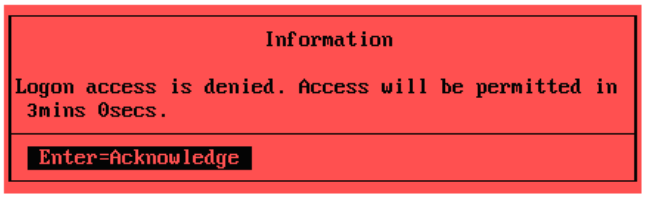
1. Type your User name (User ID).
2. Type your Password.
3. Select the relevant Windows Domain name by using the up/down arrows.
4. Press **Enter**.

The Windows desktop displays. In most common ProtectDrive configuration scenarios, the system will log the user in to Windows *automatically*. However, in isolated instances, the System Administrator may configure ProtectDrive to require the user to log in to Windows separately. Refer to Chapter 3 – Logging In to Windows.

What to Do If Your Pre-boot Login Fails

Incorrect Pre-boot Username and/or Password

If the user fails to provide ProtectDrive with a correct pre-boot user name and/or password within a pre-configured number of attempts (the default value is 3 attempts, but can be configured by the System Administrator), a lockout screen, similar to the following, displays:



When this message displays, a countdown begins and the system will be inoperable during this time (the default value is 3 minutes, but this countdown duration can also be configured by the System Administrator). Contact your System Administrator for further assistance.

Pre-boot Login Failure Due to System Inoperability

If any of the ProtectDrive system files and/or encrypted hard drive partitions experience corruption, the user may not be able to authenticate into the system at pre-boot. In these isolated instances, an error screen will display an ACS Error Number, as shown in the example below.

Communicate the error number to the System Administrator.

© SafeNet, Inc.

Chapter 3
Logging In to Windows

Typically, the ProtectDrive system will be configured by the System Administrator to *automatically* log the user in to Windows following their successful pre-boot authentication. In this case, no further user input is required, and Windows will load normally.

If however, users are required to manually login to Windows, refer to the section below.

Single sign-on is currently not supported with fingerprint login, therefore, the user will be required to log in manually. Refer to page 15 for details.

Manual Windows Login

If the System Administrator has set up the system to require users to manually log in to Windows, then one of the two Windows **Welcome** screens (similar to the ones shown below) will display immediately following the user's successful pre-boot authentication.

Figure 7 - Smart Card/Token/PIN Windows Welcome Screen

Welcome to Windows
Microsoft
Windows Server 2003
Standard Edition
Copyright © 1985-2003 Microsoft Corporation
Microsoft
Press Ctrl-Alt-Delete to begin.
Requiring this key combination at startup helps keep your computer secure. For more information, click Help.
Help

Figure 8 – User ID/Password/Domain Windows Welcome Screen

Logging In to Windows With Smart Card/Token and PIN

The Smart Card/Token/PIN users use the Windows **Welcome** screen shown in Figure 7 on the previous page.

To manually log in to Windows:

1. Insert your smart card or token into the reader. A screen similar to the following Windows *Log On* screen displays:

2. Enter your PIN.

3. Click **OK**. Windows will load normally, and then your familiar Windows desktop displays.

Logging In to Windows with User Name/Password/Domain

The User name/Password/Domain users use the Windows **Welcome** screen shown in Figure 8 on the previous page.

To manually log in to Windows:

1. Press **Ctrl-Alt-Del**. A screen, similar to the following Windows *Log On* screen, displays:

© SafeNet, Inc.

2. Enter your Windows **User name** and **Password** supplied by your System Administrator.

3. Select your Windows Domain name from the **Log on to** drop-down list.

4. Click **OK**. Windows will load normally, and then your familiar Windows desktop displays.

Logging In to Windows with Smart Card/Token and Fingerprint

Single sign-on is currently not supported with fingerprint login, which means you are not automatically logged in to Windows after you've successfully logged in to ProtectDrive.

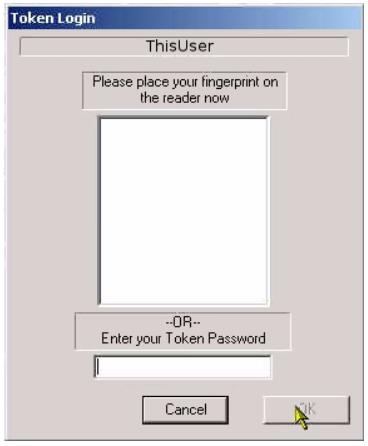
After logging in to ProtectDrive, you are immediately presented with a *Token Login* screen (shown in the following procedure), rather than the Windows *Login* screen as, shown in the previous examples. You can use fingerprint authentication, or, as an alternative, you can log in with a PIN.

If a fingerprint is used, note that the system can be configured to accept up to four fingerprints. The number of fingerprints that are "enrolled" will determine the login screen that displays. Refer to the *SafeNet Borderless Security PK and SSO User Guide* for details on fingerprint enrollment.

After successfully logging in to ProtectDrive, follow these steps.

One Fingerprint Enrolled

1. If only one fingerprint is enrolled, a *Token Login* screen, similar to the one shown below, displays. Place your finger on the reader.

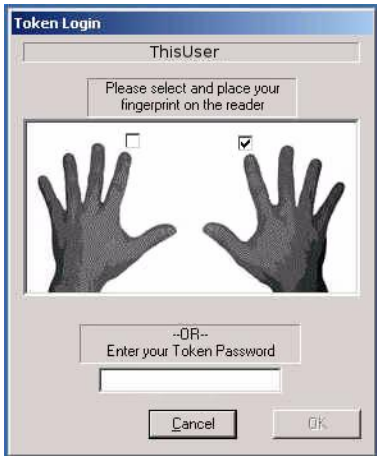


2. Follow the instructions on the screen to complete the login procedure.

3. After a successful authentication, the Windows desktop displays.

Multiple Fingerprints Enrolled

1. If more than one fingerprint is enrolled, a *Token Login* screen, similar to the one shown below, displays. The check boxes indicate the number of fingerprints that are enrolled (there are two in the example below).



   Select the check box above the fingerprint you will use to log in with, and place that finger on the reader.

2. Follow the instructions on the screen to complete the login procedure.

3. After a successful authentication, the Windows desktop displays.

© SafeNet, Inc.

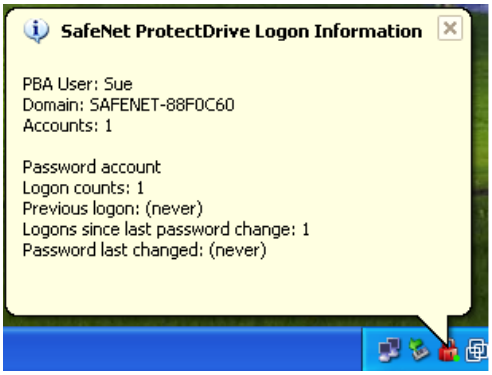
Chapter 4
Using Windows with ProtectDrive

ProtectDrive is designed to run with minimal visibility to the end user. The intent is to produce no effect on normal computer system operation. However, some minor software compatibility issues pertaining to various MS Windows programs and utilities exist and need to be taken into consideration.

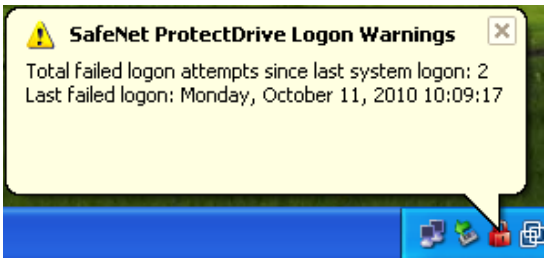
This chapter outlines various MS Windows and software compatibility-related considerations the user needs to make when operating a computer system secured by ProtectDrive.

ProtectDrive User Authentication Activity Tracking

The System Administrator may configure your system to inform you of your ProtectDrive authentication activity. If this is the case, after successful Windows authentication, and right before Windows Explorer loads, the following ProtectDrive balloon tip will display to alert the user of their ProtectDrive Pre-boot authentication activity to date.



If there have been any unsuccessful login attempts, the following ProtectDrive balloon tip will display:


SafeNet ProtectDrive Logon Warnings
Total failed logon attempts since last system logon: 2
Last failed logon: Monday, October 11, 2010 10:09:17

Disk Encryption Warning

If the system has been configured to alert users of the incomplete encryption of any of the hard disk partitions, and any of the drives are found to be unencrypted, then the following ProtectDrive balloon tip will display immediately after Windows Explorer loads:

SafeNet ProtectDrive Encryption Warning
All hard drives must be fully encrypted to ensure your system is secure.
The following drives have not been fully encrypted:
C:

If this warning displays, click **OK** and contact your System Administrator.

Windows Shrink Volume Feature

Windows Server 2008 includes a Disk Management "Shrink Volume" feature which allows you to shrink an existing partition or volume. This feature is incompatible with ProtectDrive, as the addition or removal of drives or partition changes are not supported after ProtectDrive is installed. Changing the size of a partition using this feature, or any other means is not supported by ProtectDrive and will lead to problems.

SafeNet ProtectDrive Notification Area Icon

The Windows *notification area* is a portion of the taskbar that displays system and program notifications and status. If ProtectDrive has been configured with the **Show SafeNet ProtectDrive System Tray Icon** option enabled (in **PD Settings > Advanced > User Interface**), a small ProtectDrive icon is placed in the Windows notification area of the taskbar, located in the lower-right corner of the Windows desktop. The icon indicates that the PC is secured by ProtectDrive.

During ProtectDrive-related operations, the icon displays a green dot in the lower-right corner, to notify the user that an action is underway. This is which is especially helpful during potentially lengthy or system resource-hungry tasks. ProtectDrive-related operations include:

- Activating or deactivating pre-boot authentication
- Encrypting or decrypting fixed and removable drives
- Processing remote configuration updates

© SafeNet, Inc.

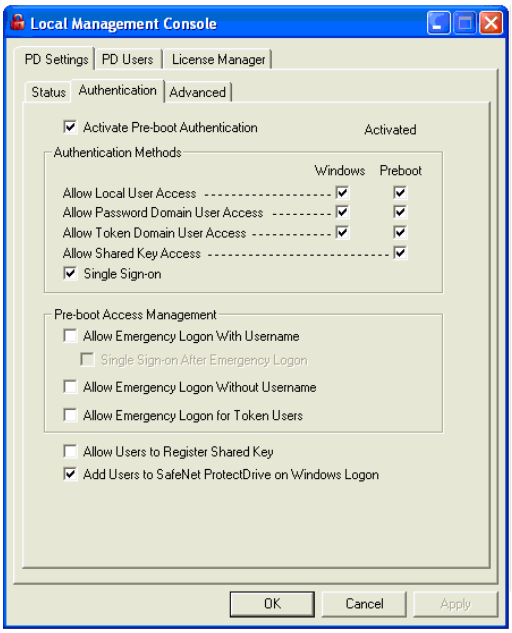
Hover the mouse pointer over the ProtectDrive icon to display a tooltip of the task that is in progress. The following example shows a tooltip for the encryption process of drive C.

If the **Show SafeNet ProtectDrive System Tray Icon** option is not enabled, then the ProtectDrive icon will not display at all.

Right-click on the ProtectDrive icon to access the *Local Management Console*, which allows you to lock the Windows desktop (not available if ProtectDrive is installed on Windows Vista), register/manage a user's shared key (if this option is configured), and view information about SafeNet ProtectDrive (version number, license, and copyright information).

Access the Local Management Console

1. Right-click on the icon in the notification area.
2. Select **Local Management Console**.



You can also open the *Local Management Console* by double-clicking on the icon, or you can access it from the Windows Start menu. Select **Start > Programs > SafeNet ProtectDrive > Local Management Console**.

Typically, the **PD Settings** are configured by the System Administrator. For details on these settings, refer to the *SafeNet ProtectDrive Administration Guide*.

The *Local Management Console* **PD Settings** and **PD Users** tabs on a remotely-managed client are accessible, but they are read-only.

Lock the Windows Desktop

This feature is not available if ProtectDrive is installed on Windows Server 2008.

1. Right-click on the icon in the notification area.
2. Select **Lock Computer**. The Windows screen will display a icon to indicate it is now locked.
3. Insert your smart card/token or press **Ctrl-Alt-Del** to log back in to the Windows desktop.

Register a Shared Key

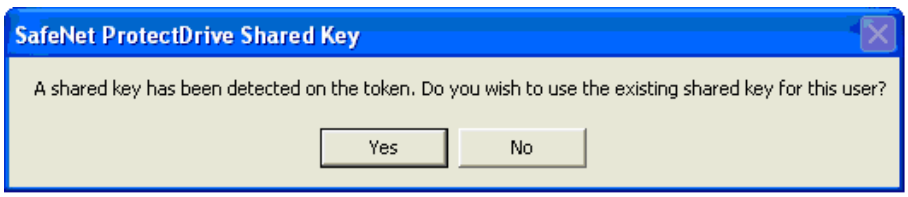
If the **Allow Users to Register Shared Key** option is enabled (**PD Settings > Authentication**), then the **Shared Key** selection displays in the SafeNet ProtectDrive system tray icon menu.

To use a shared key token for pre-boot authentication, a user must have a shared key registered to them.

Follow these steps if the token user <u>does not have</u> a previously assigned shared key:

1. Insert the token and right-click on the icon in the notification area.
2. Select **Shared Key**. The following screen displays:

3. Enter the token user's PIN, and then click **OK**.
4. If a shared key *already exists* on the token, the following message displays:


SafeNet ProtectDrive Shared Key
A shared key has been detected on the token. Do you wish to use the existing shared key for this user?
Yes
No

© SafeNet, Inc.

- If you choose **Yes**, the existing shared key is registered to the user and the following message displays:

Click **OK** to complete the procedure.

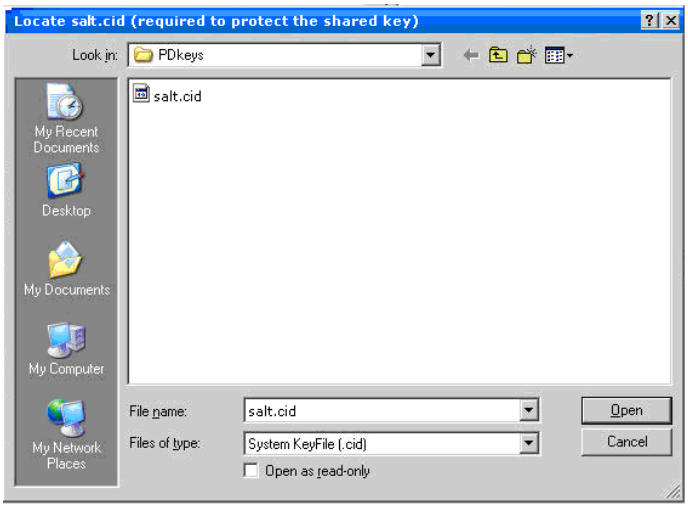
- If you choose **No**, the following message displays:

  - If you choose **Yes** to overwrite the shared key on the token, a new shared key is generated for the user on the token.

    - If you are configuring the shared key on the **client**, the following message will display to indicate that the key has been updated:

Click **OK** to complete the procedure.

➢ If you are configuring the shared key from the ProtectDrive **server**, you are prompted for the **salt.cid** file.



Navigate to and select the **salt.cid** file and then click **Open**. The following message will display to indicate that the key has been updated:

Click **OK** to complete the procedure.

- If you choose **No** to not overwrite the shared key, the process is cancelled. A new shared key is not created or assigned to the user.

© SafeNet, Inc.

Follow these steps if the token user has a previously assigned shared key:

1. Insert the token and right-click on the icon in the notification area.
2. Select **Shared Key**. The following screen displays:

Shared Key Exists
The user has an existing shared key.
Select remove to disable this user logging on with this shared key.
Select replace to change this user's shared key.
Replace
Remove
Cancel

- If you choose **Replace**, follow the steps in the previous section (on page 20), starting with step 3.
- If you choose **Remove**, the existing shared key is unassigned/removed from the ProtectDrive user's profile. The following screen displays:

Click **OK** to complete the procedure.

View *About SafeNet ProtectDrive* Information

1. Right-click on the icon in the notification area.
2. Select **About SafeNet ProtectDrive**. A screen similar to the following will display:

About SafeNet ProtectDrive
SafeNet ProtectDrive 9.4.0.17
OK
Base license
Normal Standalone (Valid)
Feature license(s)
Removable Media (Valid)
Remote Configuration (Valid)
SafeNet
www.safenet-inc.com
Copyright 2011 SafeNet, Inc. All rights reserved. SafeNet and ProtectDrive are either registered trademarks of SafeNet Incorporated in the United States and/or other countries.

Using the Windows Folder Compression Application on Your ProtectDrive-secured PC

Windows folder compression is fully supported, but with one exception: The ProtectDrive system files directory (*Securdsk)* must not be compressed on any partition.

Do not install ProtectDrive to a compressed system drive if the system drive is C: only. This will result in the compression of the *C:\Securdsk* directory, which will interfere with normal ProtectDrive operations.

Using the Windows System Restore Utility on Your ProtectDrive-secured PC

Windows system restore points that were created *prior to* installing ProtectDrive are rendered useless. The system can only be restored to a restore point that is created *after* installing ProtectDrive.

Changing Your ProtectDrive Pre-boot Password

1. Press **Ctrl-Alt-Del** and select **Change Password**.

2. Select the appropriate domain from the **Log on to** drop-down list and specify the new password.

   For local Windows, the new password change becomes effective immediately. See **(this computer)** shown in the screen below.

© SafeNet, Inc.

For Windows Domain (shown in the screen to the right), the user will need to log out of Windows and log back in. This will propagate the new password to the ProtectDrive Pre-boot User database.

If the user does not follow this procedure, they will have to use their old password at pre-boot. Once they log in to Windows Domain with their new password, this new password will propagate to the ProtectDrive Pre-boot User database.

Disallowed Device Access Errors

The System Administrator can configure the system to disallow user access to specific devices, such as ports or removable media (these changes would take effect after reboot only). If a user, whose device access control permissions are disabled, attempts to access a certain device, a message, similar to the following, will display.

If this occurs, the user should contact their System Administrator for further assistance.

Device access control permissions are discussed on page 43.

Backing Up the License File

In the event that your hard drive requires reformatting or re-imaging after ProtectDrive has been installed, you'll need the existing ProtectDrive license file to re-install on the same machine. If you do not have a backup copy of the existing license file, you will be required to contact SafeNet for a new license file for the same machine, which could take longer to get the machine back up and running.

After ProtectDrive has been installed, follow these steps to preserve the ProtectDrive license file. It should be stored in a safe location for future use, if it is ever necessary.

1. Go to *C:\Program Files\SafeNet ProtectDrive*.
2. Copy the **lservrc** file and save it to a safe location, preferably on another drive or computer (since you will be formatting this drive).
3. Rename the **lservrc** file to **license.txt**.

Use this **license.txt** file when you re-install ProtectDrive on the same machine. For installation details, refer to the *ProtectDrive Administration Guide*.

THIS PAGE INTENTIONALLY LEFT BLANK

© SafeNet, Inc.

Chapter 5
Encrypting Hard Drives & Removable Media

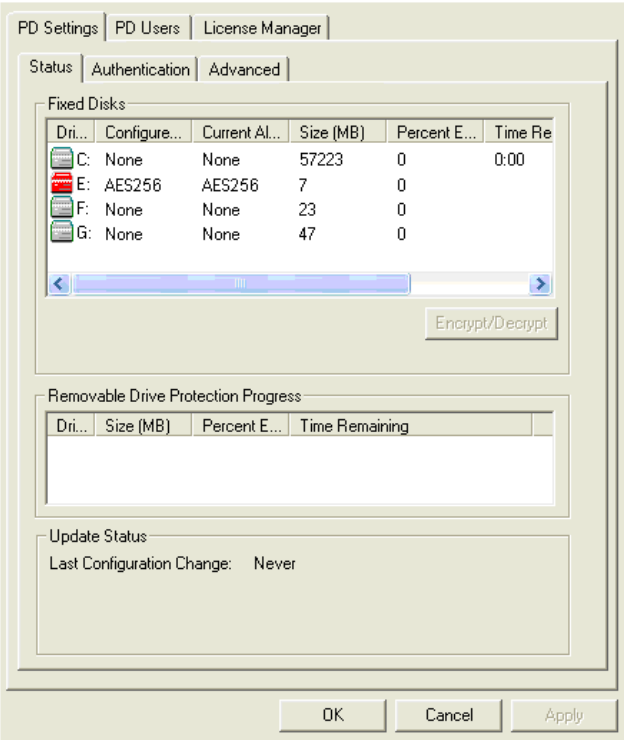
Encrypt a Hard Drive

To initially encrypt a hard drive, perform the following steps:

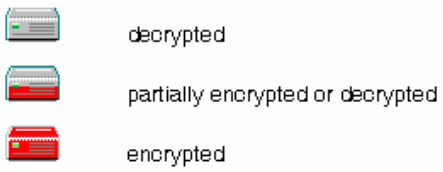
1. From the Windows desktop, select **Start > Programs > SafeNet ProtectDrive > Local Management Console**.

2. Click the **PD Settings** tab.

3. Click the **Status** tab.



The following icons represent the drive's status:



The columns that display are:

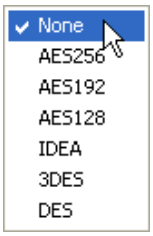
Drive	Partition drive letter
Configured Algorithm	Algorithm selected for encryption of the given partition
Current Algorithm	All encrypted partitions will display the algorithm used for their encryption
Size (MB)	The size of the partition
Percent Encrypted	Status indicator during ongoing encryption operation
Time Remaining	Status indicator during ongoing encryption operation

4. Click on the drive to encrypt. To choose more than one drive to encrypt:

   - Press **Ctrl+mouse-click** to choose multiple, non-consecutive drives.
   - Press **Shift+mouse-click** to choose a block of consecutive drives.

   If multiple drives are selected, they will **all** be encrypted sequentially (one after the other) with the same algorithm that is selected in step 5 below. However, when needed, you can change an encryption algorithm on a drive. Refer to *Re-encrypt a Drive Using a Different Algorithm* on page 30.

5. Click **Encrypt/Decrypt** and choose an encryption algorithm from the list that displays.



The algorithm selections that can display will depend on your system configuration (meaning, some selections may be unavailable). Consult your System Administrator for guidance on which encryption algorithm best suits your system.

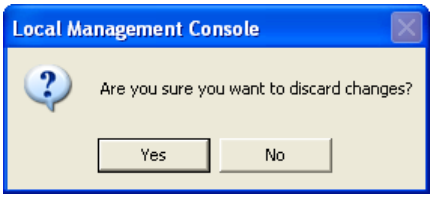
The **IDEA**, **3DES**, and **DES** algorithm selections are not available if FIPS mode is enabled.

© SafeNet, Inc.

None	This selection will cause an encrypted drive to be decrypted. Hard drive decryption is only allowed for System Administrators. This setting is disabled for users without administrative privilege.
AES256 **AES192** **AES128**	The AES256 (Advanced Encryption Standard) selection is a symmetric block cipher that processes 256-bit keys. ProtectDrive uses the cipher in CBC mode.
IDEA	The International Data Encryption Algorithm (IDEA) cipher operates using 64-bit blocks and 128-bit keys. ProtectDrive uses the cipher in CBC mode.
3DES	The Triple DES cipher is a publicly tested 112-bit key 64-bit block cipher. ProtectDrive uses the cipher in CBC mode. Details on the cipher are publicly available from many sources.
DES	The DES cipher is a publicly tested 56-bit key 64-bit block cipher. ProtectDrive uses the cipher in CBC Mode. Details on the cipher are publicly available from many sources.

6. Click **Apply** or **OK**.

   - If you click **Apply**, the encryption process begins, and the *Local Management Console* remains open.
   - If you click **OK**, the encryption process begins, and the *Local Management Console* closes.
   - If you click **Cancel**, the following prompt displays:



   - If you click **Yes** to proceed, the encryption process is cancelled (no encryption will occur) for any partition where encryption has not yet begun.
   - If you click **Yes** while an encryption process is already in progress on a partition, then encryption will proceed on that partition. You can decrypt it after encryption has completed.

The **OK** and **Apply** buttons are disabled if the System Administrator configured ProtectDrive to disallow disk encryption.

Decrypt a Drive

Decrypting a hard drive can only be performed by the System Administrator. If you do not have administrative privileges, this option is not available to you.

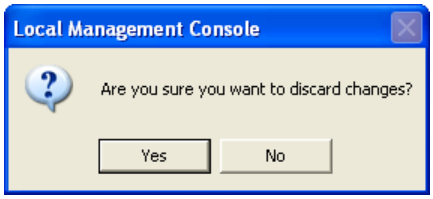
1. From the Windows desktop, select **Start > Programs > SafeNet ProtectDrive > Local Management Console**.
2. Click the **PD Settings** tab.
3. Click the **Status** tab.
4. Click on the drive to decrypt.
5. Click **Encrypt/Decrypt** and select **None**.
6. Click **OK** or **Apply**. The drive will be decrypted.

Re-encrypt a Drive Using a Different Algorithm

If a drive is already encrypted, you can re-encrypt it with a different algorithm any time. In this case, the selected drive will be decrypted first, and then it will be re-encrypted with the newly selected algorithm. If multiple drives are selected for decryption, they are decrypted sequentially, one at a time, and then re-encrypted sequentially.

1. From the Windows desktop, select **Start > Programs > SafeNet ProtectDrive > Local Management Console**.
2. Click the **PD Settings** tab.
3. Click the **Status** tab.
4. Click on the drive to re-encrypt.
5. Click **Encrypt/Decrypt** and select an alternative algorithm.
6. Click **OK** or **Apply**. The drive will be re-encrypted with the newly selected algorithm.

    - If you click **Cancel**, the following prompt displays:



© SafeNet, Inc.

- If you click **Yes** to proceed, the re-encryption process is cancelled for all partitions where re-encryption has not yet begun (it will remain encrypted with the previously selected algorithm).
- If you click **Yes** while the re-encryption process is already in progress on a partition, then re-encryption will proceed on that partition.

Removable Media

This section describes all of the features available for removable media. Most removable media features—encryption, decryption, locking, and unlocking— are available through Windows Explorer. Not every user will have access to these features, as their permissions will depend on how System and User policies were configured by the System Administrator.

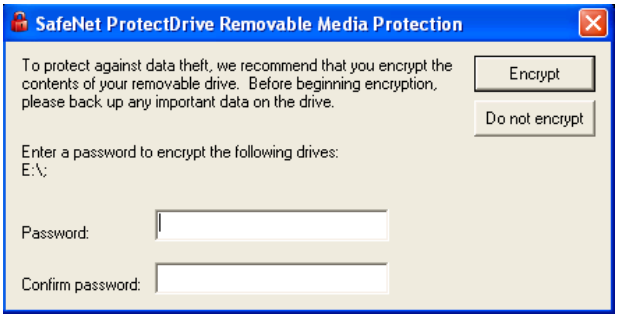
A password is required to encrypt, unlock, and decrypt removable media.

Encrypt Removable Media

Your system can be configured to *automatically* prompt users to decide whether or not to encrypt the removable media as soon as the system detects it. Additionally, users can opt to encrypt a removable media device at any time through the *Windows Explorer* options described on the following pages.

Automatic Prompt to Encrypt

If the system is configured to automatically detect unprotected removable media when it is connected, the following prompt displays:


SafeNet ProtectDrive Removable Media Protection
To protect against data theft, we recommend that you encrypt the contents of your removable drive. Before beginning encryption, please back up any important data on the drive.
Encrypt
Do not encrypt
Enter a password to encrypt the following drives:
E:\;
Password:
Confirm password:

1. Enter and confirm the encryption password that will be required to access this device and click **Encrypt**. (If you click **Do not encrypt**, you may not have access to the unprotected media. This will depend on whether the System Administrator granted you permission to access unprotected media.)

2. Click **OK**. A progress bar will display during the encryption.

3. Click **OK** when the following completion prompt displays:

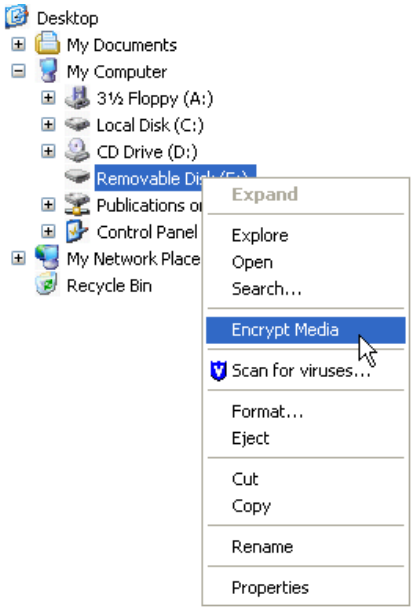
From this point forward, the encryption password will be required to unlock or decrypt the device.

Windows Explorer Encrypt Media Option

You can manually choose to encrypt removable media through Windows Explorer.

1. Navigate to the removable media device in Windows Explorer.

2. Right-click on the device, and then choose **Encrypt Media**.



© SafeNet, Inc.

3. Enter and confirm the encryption password to access the device, and then click **Encrypt**.

SafeNet ProtectDrive Removable Media Protection
To protect against data theft, we recommend that you encrypt the contents of your removable drive. Before beginning encryption, please back up any important data on the drive.
Encrypt
Do not encrypt
Enter a password to encrypt the following drives:
E:\;
Password:
Confirm password:

4. Click **OK** when the following completion prompt displays.

From this point forward, the encryption password will be required to unlock or decrypt the device.

Lock Removable Media

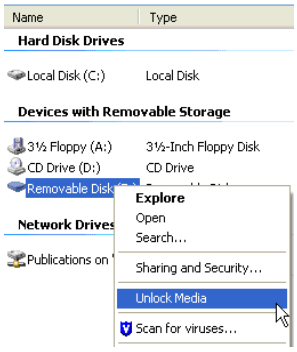
Use the Windows Explorer **Lock Media** option to disallow unauthorized users access to selected removable media that is still connected. An encryption password is required to *unlock* the media.

1. Navigate to the removable media device in Windows Explorer.
2. Right-click on the device to lock, and then choose **Lock Media.**

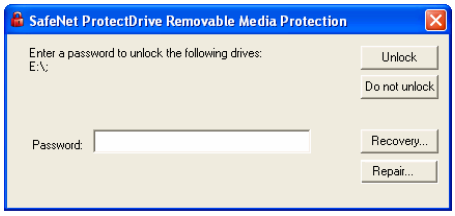
Unlock Removable Media

Use the Windows Explorer **Unlock Media** option to allow access to the selected media. An encryption password is required.

1. Navigate to the removable media device in Windows Explorer.
2. Right-click on the device to be unlocked, and then choose **Unlock Media.**



3. When prompted, enter the encryption password, and then click **Unlock**.



© SafeNet, Inc.

Decrypt Removable Media

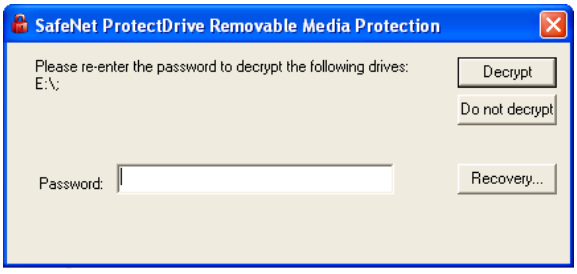
If the system is configured to allow users to decrypt removable media, use the Windows Explorer **Decrypt Media** option. A password is required to use this option, and the device must be **unlocked** before it can be decrypted.

1. Navigate to the removable media device in Windows Explorer.

2. Right-click on the device to decrypt, and then select **Decrypt Media**.

3. Click **Yes** to confirm decryption.

4. When prompted, enter the encryption password, and then click **Decrypt**.



5. Click **OK** when the completion prompt displays:

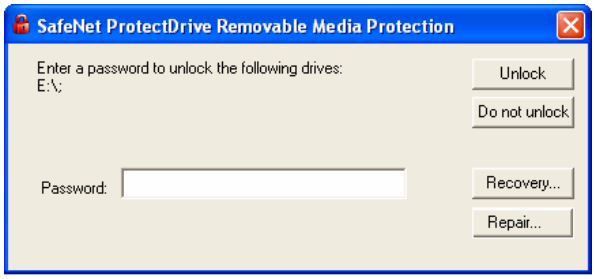
Repair Removable Media

Standard Recovery Procedure

To ensure the recovery and reusability of a removable media device should it become unstable or compromised, follow this procedure to repair the device (remove encryption), and then reformat it for reuse.

This procedure should be performed for each USB flash drive that is deployed.

1. Connect the removable media to the PC. The following screen should display when the device is detected.



2. Click **Repair**.

3. Click **OK** when the following message displays:

SafeNet ProtectDrive Removable Media Protection
The encrypted status can be removed so that the drive can be formatted and usable. This will result in data loss!
Would you like SafeNet ProtectDrive to remove the encrypted status of the drive?
Yes
No

4. Click **Yes**.

© SafeNet, Inc.

5. When prompted, click **OK**, and then safely remove the device.

SafeNet ProtectDrive Removable Media Protection
Please remove drive E:\ and re-insert it. Then format the drive to make it usable.
OK

6. Re-connect the removable media device to reformat it for reuse. Reformatting should be done before the device is re-encrypted.

Alternate Recovery Procedures

In the event that the *Standard Recovery Procedur*e described above does not return the device to a reusable state, there are two alternate recovery procedures that a System Administrator can use.

These alternate procedures—*Use RmRMBR* and *Use Sector 0 Backup Data*—are detailed in Chapter 5 of the *ProtectDrive Administration Guide*.

Contact SafeNet Support prior to attempting either of these procedures.

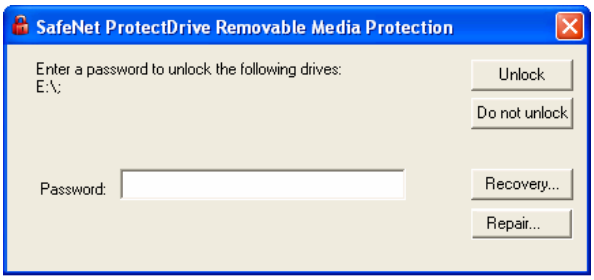
Recover Removable Media

Use this procedure to gain temporary, emergency access to the removable media in the event that a user forgets their password.

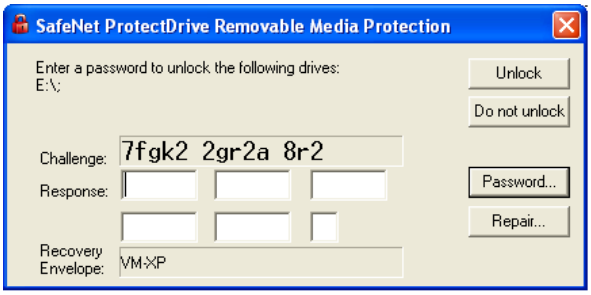
Emergency access means the user is able to perform only the functions that do **not** require a password. To regain full access to the removable media, the device will require decryption and re-encryption to reset the password. (All of these steps are included in this section.)

End User Instruction—Generate a Challenge Code

1. Connect the removable media to the PC. The following screen should display when the device is detected.



2. Click **Recovery**. A **Challenge** code displays, shown in the example below.



3. Contact your System Administrator (either in person or by phone) and provide them with the **Challenge** code.

4. The System Administrator will run the **rpadmin** utility and generate a response based on the **Challenge** code (detailed steps are on the next page), and will provide you with a recovery code. Enter this code into the **Response** field.

5. Click **Unlock.** The removable media should be temporarily available until the user removes it, at which point a new password will be required. You will have to decrypt the device to reset the password. For details, refer to page 40.

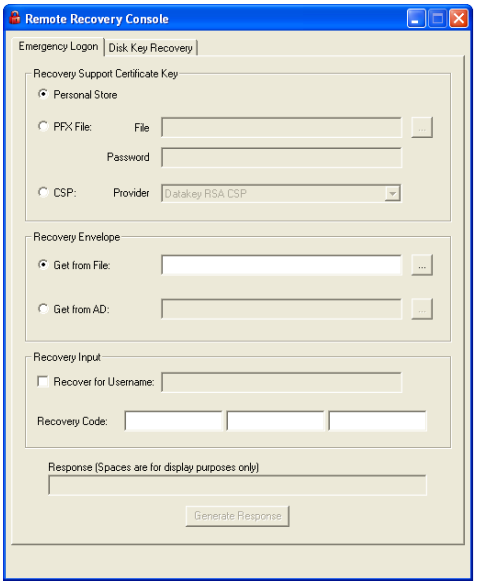
© SafeNet, Inc.

System Administrator Instruction—Generate a Recovery Response Code

The *Removable Media Key Recovery* procedure for system administration purposes is described below.

1. Run **rpadmin.exe**, located in *\Program Files\SafeNet ProtectDrive* on the server. The ProtectDrive *Remote Recovery Console* window displays.

2. Click the **Emergency Logon** tab.



3. Select the appropriate **Recovery Support Certificate Key** option:

   - **Personal Store**—If you select this option, you must have the user's private recovery key certificate copied from their Personal Store to your machine.

   - **PFX File**— If you select this option, click ..., and then browse to and open the user's private **PdRecovery.pfx** file. Enter the password.

   - **CSP**—If you select this option, choose the appropriate **Provider** from the drop-down list where the certificate key is stored.

4. Select the **Recovery Envelope** file for the user's computer:

   - **Get From File**— If you select this option, click ..., and then browse to and open the **<computername>_RecoveryEnvelope.env** file.

   - **Get From AD**—If you select this option, click ..., and then browse to the Active Directory computer and locate the computer object.

5. Enter the **Challenge** code provided by the user into the **Recovery Code** field, and then click **Generate Response**.

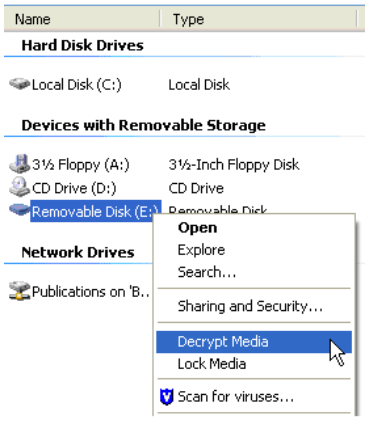
6. Instruct the user to enter the automatically-generated response code into their **Response** field, and then click **Unlock**. The removable media should be temporarily available until the user removes it, at which point the user must repair the removable media (see page 36), and then a new password will be required once the RM is reusable.

   Refer to the next sections for steps on how to reset the password.

End User Instruction—Reset the Removable Media Password

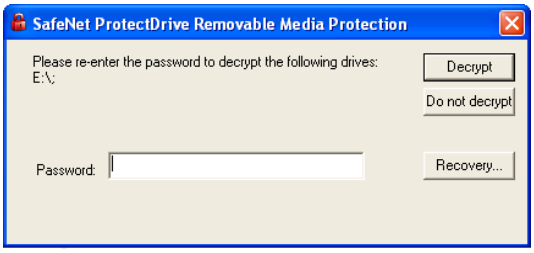
1. Safely remove and then re-connect the removable media device. Navigate to this device in Windows Explorer.

2. Right-click on the device to decrypt, and then select **Decrypt Media**.



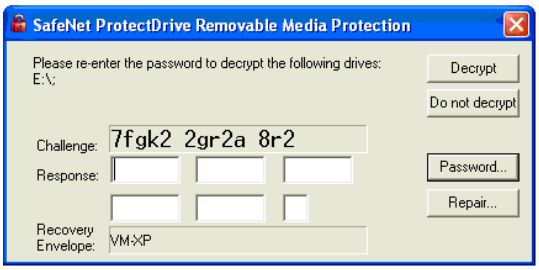
3. Click **Yes** to confirm decryption.

4. When prompted, enter the encryption password, and then click **Decrypt**.



© SafeNet, Inc.

5. Click **Recovery**. A **Challenge** code displays, shown in the example below.



6. Contact your System Administrator (either in person or by phone) and provide them with the **Challenge** code.

7. The System Administrator will run the **rpadmin** utility and generate a response (see page 38) based on the Challenge code, and will provide you with a recovery code. Enter this code into the **Response** field.

8. Click **Decrypt**.

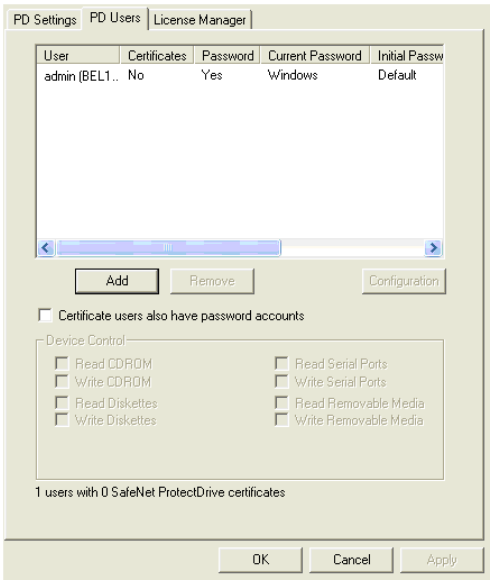
9. Click **OK** when the following completion prompt displays:

10. Safely remove and then re-connect the removable media device. Enter and confirm the new password, and then click **Encrypt**.

11. Follow the remaining prompts until encryption is complete.

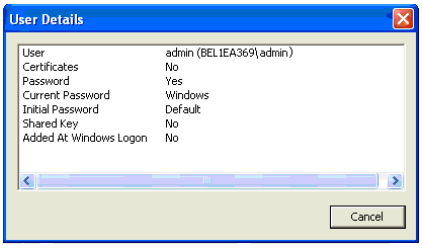
Chapter 6
Configuring ProtectDrive Users

The **PD Users** tab lists all of the users who are currently in the Pre-boot user database. Additional ProtectDrive users can be added if they are first added as a Windows user or group. From the **PD Users** tab, you can also set device access control permissions for a user, configure a user's account, set the initial default password for a user, or remove a user.



A user must have administrative privileges to change these settings.

To view a user's current settings at a glance, double-click on their name. The *User Details* window displays.



© SafeNet, Inc.

If pre-boot activation is deactivated and then reactivated, ProtectDrive resets all user passwords to the configured initial pre-boot password. (The initial pre-boot password can be explicitly defined in **PD Settings > Advanced > Password Policy**, where the default password can be set to be equal to the username, or set to a designated default. The preset default is "*password*."). A user must have administrative privileges to change these settings.

Set Device Access Control Permissions for a User

1. From the Windows desktop, select **Start > Programs > SafeNet ProtectDrive > Local Management Console**.
2. Click the **PD Users** tab.
3. Click on a user's name.
4. Select the appropriate read/write *Device Control* permissions for the user, and then click **Set**.
5. Click **Apply**, and then **OK**.

Add a ProtectDrive User

1. From the Windows desktop, select **Start > Programs > SafeNet ProtectDrive > Local Management Console**.
2. Click the **PD Users** tab.
3. (Optional) Select the **Certificate users also have password accounts** check box if you want to allow all users listed here to have pre-boot access with the use of the default password (as defined by the **Default Password** in the **PD Settings > Advanced > Password Policy** group).
4. Click **Add**.
5. Enter the local user or group name to add, and then click **OK**.
6. (Optional) If the user also has a shared key account, highlight the new user, and then click **Configuration**. Select the **User has shared key account** check box, and then click **OK**.

Change a ProtectDrive User's Initial Password

1. From the Windows desktop, select **Start > Programs > SafeNet ProtectDrive > Local Management Console**.
2. Click the **PD Users** tab.
3. Click on a user's name, and then click **Configuration**.
4. Enter and confirm the user's initial pre-boot password, and then click **OK**.

If the **Use default password** option is selected on the **User Account Configuration** screen, de-select this option to change the user's initial pre-boot password.

Remove a ProtectDrive User

1. From the Windows desktop, select **Start > Programs > SafeNet ProtectDrive > Local Management Console**.
2. Click the **PD Users** tab.
3. Click on a user's name, and then click **Remove**.
4. Click **OK** to confirm the deletion.

© SafeNet, Inc.

Chapter 7
Troubleshooting

What to Do If You Misplace Your Smart Card/Token or Forget Your PIN

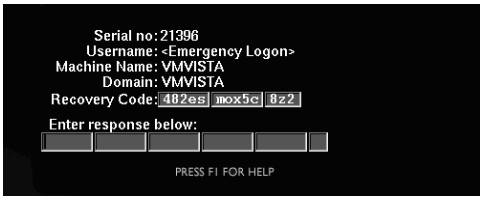
This procedure is for *smart card/token/PIN/fingerprint* users.

If you misplace your smart card/token or forget your PIN, access to the system may be achieved by performing the following ProtectDrive *Emergency Logon for Token Users* procedure (at the discretion of the System Administrator).

1. Place the cursor in the **PIN** field, and then press **Shift+F9**.

or

The following recovery/response screen displays.



2. Contact your System Administrator (either in person or by phone) and provide them with the displayed *Recovery Code (Challenge)*.

3. The System Administrator will provide you with the *Response Code*. Enter this code into the **Enter response below** field shown below.

4. At this point, Windows will proceed to load normally and will either log you in to Windows *automatically* or *manually*, depending on how the System Administrator configured ProtectDrive.

   For manual Windows log on, please review Chapter 3 – Logging On to Windows.

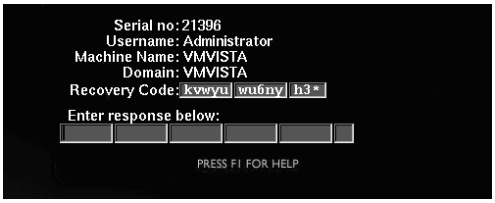
What to Do If You Forget Your Password

This procedure is for *user ID/password/domain* users.

If you forget your password, the *Emergency Logon With Username Procedure* can be used to gain access to the system.

1. Enter your username into the **User ID** field of the *Username/Password/Domain Name Log On* screen, shown below.

2. Place the cursor in the **Password** field and press **Shift+F10.** The following recovery/response screen displays.



© SafeNet, Inc.

3. Contact your System Administrator and provide them with the displayed *Recovery Code* (*Challenge*) along with your *Username*.

4. The System Administrator will provide you with the *Response Code*. Enter this code into the **Enter response below** field.

5. At this point, Windows will proceed to load normally and will either log you on to Windows *automatically* or *manually*, depending on how the System Administrator configured ProtectDrive.

   For manual Windows log on please review Chapter 3 – Logging On to Windows.

What to Do If You Do Not Have a Pre-boot User Account

This procedure is for *username/password/domain name* users.

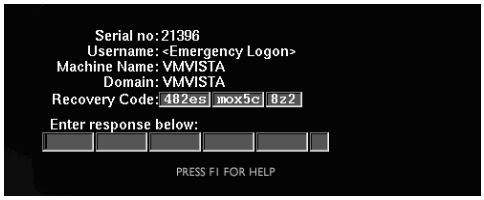
If you have not yet had the opportunity to log on to your ProtectDrive secured PC, you may be required by the System Administrator to execute the following *Emergency Logon Without Username Procedure* during your first-time-ever system log on.

This procedure applies only to the *Username/Password/Domain Name* authentication method. New *smart card/token/PIN* users have new pre-boot accounts already created for them by the System Administrator and, therefore, are able to log in to the system without undergoing any additional procedures such as the one described in this section.

Emergency Logon Without Username Procedure

1. Place the cursor in the **User ID** field of the *Username/Password/Domain Name Log On* screen shown below, and then press **Shift+F9**.

   The following recovery/response screen displays.



2. Contact your System Administrator and provide them with the displayed *Recovery Code (Challenge)*.

3. In return, the System Administrator will provide you with the *Response Code*. Enter this code into the **Enter response below** field.

   One-time-only pre-boot access to the system is granted.

4. At this point, proceed to normal Windows login. Your next system login will be as described in Chapter 2 – Logging On to Your ProtectDrive Secured PC.

© SafeNet, Inc.

END OF DOCUMENT